
6.4 Page-Level Protection

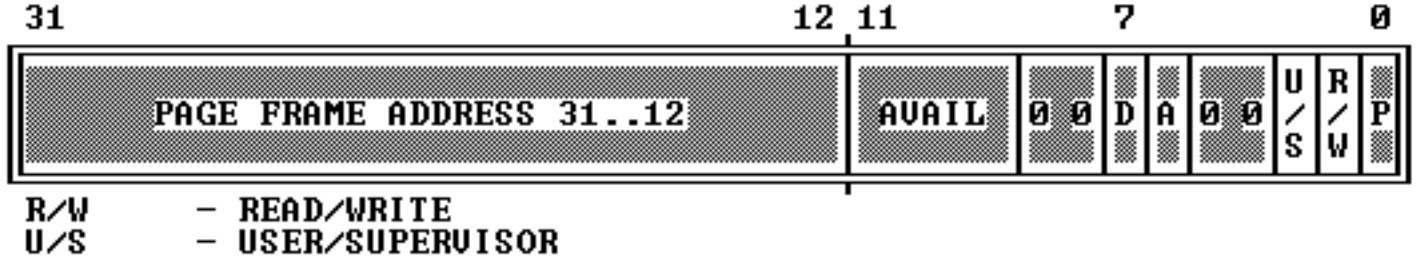
Two kinds of protection are related to pages:

1. Restriction of addressable domain.
2. Type checking.

6.4.1 Page-Table Entries Hold Protection Parameters

Figure 6-10 highlights the fields of PDEs and PTEs that control access to pages.

Figure 6-10. Protection Fields of Page Table Entries



6.4.1.1 Restricting Addressable Domain

The concept of privilege for pages is implemented by assigning each page to one of two levels:

1. Supervisor level (U/S=0) -- for the operating system and other systems software and related data.
2. User level (U/S=1) -- for applications procedures and data.

The current level (U or S) is related to CPL. If CPL is 0, 1, or 2, the processor is executing at supervisor level. If CPL is 3, the processor is executing at user level.

When the processor is executing at supervisor level, all pages are addressable, but, when the processor is executing at user level, only pages that belong to the user level are addressable.

6.4.1.2 Type Checking

At the level of page addressing, two types are defined:

1. Read-only access (R/W=0)
2. Read/write access (R/W=1)

When the processor is executing at supervisor level, all pages are both readable and writable. When the processor is executing at user level, only pages that belong to user level and are marked for read/write access are writable; pages that belong to supervisor level are neither readable nor writable from user level.

6.4.2 Combining Protection of Both Levels of Page Tables

For any one page, the protection attributes of its page directory entry may differ from those of its page table entry. The 80386 computes the effective protection attributes for a page by examining the protection attributes in both the directory and the page table. Table 6-5 shows the effective protection provided by the possible combinations of protection attributes.

6.4.3 Overrides to Page Protection

Certain accesses are checked as if they are privilege-level 0 references, even if CPL = 3:

- LDT, GDT, TSS, IDT references.
- Access to inner stack during ring-crossing CALL/INT.

---

up: Chapter 6 -- Protection
prev: 6.3 Segment-Level Protection
next: 6.5 Combining Page and Segment Protection